

Title (en)
ENCRYPTED SEARCH IN A DATABASE

Title (de)
VERSCHLÜSSELTE SUCHE IN EINER DATENBANK

Title (fr)
RECHERCHE CHIFFRÉE DANS UNE BASE DE DONNÉES

Publication
EP 3958157 A1 20220223 (DE)

Application
EP 21192120 A 20210819

Priority
DE 102020121984 A 20200821

Abstract (de)
Die Erfindung betrifft ein Verfahren für eine verschlüsselte Suche in einer Datenbank (125) mit einer auf einem Server (100) bereitgestellten durchsuchbaren, verschlüsselten Indexstruktur (108). Die Indexstruktur (108) umfasst einen ersten Index (111), welcher eine erste Aufstellung (110.1) der von den Datensätzen der Datenbank (125) umfassten Datenelemente umfasst. Die Datenelemente des ersten Index (111) sind jeweils unter Verwendung eines ersten kryptographischen Schlüssels verschlüsselt. Die Indexstruktur (108) umfasst ferner einen zweiten Index (113), welcher eine zweite Aufstellung (110.2) der von den Datensätzen der Datenbank (125) umfassten Datenelemente umfasst. Die Datenelemente des zweiten Index (113) sind jeweils unter Verwendung eines zweiten kryptographischen Schlüssels verschlüsselt und ihnen sind jeweils erste Angaben (112) zugeordnet, aus welchen sich eine Häufigkeit des Auftretens der entsprechenden Datenelemente in der Datenbank (125) ergibt. Die Indexstruktur (108) umfasst ferner einen dritten Index (115), welcher eine dritte Aufstellung (110.3) der von den Datensätzen der Datenbank (125) umfassten Datenelemente umfasst. Die Datenelemente des dritten Index (115) sind jeweils unter Verwendung eines dritten kryptographischen Schlüssels verschlüsselt und ihnen sind jeweils zweite Angaben (114) zugeordnet sind, welche jeweils in adressierbarer Weise die Datensätze identifizieren, in denen die Datenelemente jeweils gespeichert sind.

IPC 8 full level
G06F 21/62 (2013.01)

CPC (source: EP)
G06F 21/6218 (2013.01); **G06F 21/6227** (2013.01)

Citation (search report)

- [XAYI] EP 3388969 A1 20181017 - DSWISS AG [CH]
- [IAY] EP 3364316 A1 20180822 - VISA INT SERVICE ASS [US]
- [A] WO 2018104275 A1 20180614 - BUNDESDRUCKEREI GMBH [DE]
- [A] BOUCENNA FATEH ET AL: "Secure Inverted Index Based Search over Encrypted Cloud Data with User Access Rights Management", JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, SPRINGER SINGAPORE, SINGAPORE, vol. 34, no. 1, 18 January 2019 (2019-01-18), pages 133 - 154, XP036685920, ISSN: 1000-9000, [retrieved on 20190118], DOI: 10.1007/S11390-019-1903-2

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
EP 3958157 A1 20220223; DE 102020121984 A1 20220224

DOCDB simple family (application)
EP 21192120 A 20210819; DE 102020121984 A 20200821